Federal Computer Incident Response Center

The FedCIRC Bits & Bytes

A quarterly newsletter for Information System Security Managers/Officers & System Administrators

January 1, 2002 Volume III, Issue 1

TechNotes

Port Scans, Should they be reported: Yes or No

Many organizations and individuals are asking if they should report port scans or just disregard them. Before the issue is discussed, we should have a clear understanding of what is meant by the term “port scan”. Using a physical world comparison, port scanning is similar to an individual physically checking to see if the doors and windows of houses are locked, and possibly noting the type of lock used. In the cyber world, the individual is checking to see what ports are open and what services (including versions) are running on a system or systems. It is usually hard to tell if a particular port scan incident is simply a case of individual curiosity or a precursor to an attempted attack. However, there are some clues that can provide one with an idea of the scanner’s intentions. If your router, IDS, and/or firewall logs show scans against multiple systems for multiple ports, the potential attacker is gathering information (albeit noisily) that may be used in a subsequent attack. If the logs show scans of one or more systems for only a few ports or only one port, an attack is even more likely to follow; the attacker is looking for systems that are susceptible to a particular vulnerability in a service known to run on a specific port. SANS recently released a list of the Top 20 Vulnerabilities, which included commonly probed ports (document is available at http://www.sans.org/top20.htm). Scans against these ports are often followed by actual attacks (especially if the service running on these ports is susceptible to a known vulnerability). Other frequently probed ports (not included in the SANS document) include: 31337 (used by Back Orifice), 1243 (SubSeven), and 12345 (NetBus).

Since port scanning by itself is not considered a crime in most principalities, very few individuals bother to hide their activity. However, if the scans are reported to Incident Response Teams (IRT) such as FedCIRC, these teams can analyze the reports to possibly correlate IP addresses or port numbers across multiple systems. Single events may not appear significant, but when taken collectively they may indicate evidence that a major incident is occuring or the emergence of a new vulnerability; this information can be used proactively to stop attacks before significant damage is done. Therefore, FedCIRC requests that you report all scans to assist us in protecting the health of the Federal Information Infrastructure; please send these reports to fedcirc@fedcirc.gov and begin the subject line with the text [SCAN].

FedCIRC encourages all users to review these five simple solutions to minimize the impact of SYN Flood Denial of Service attacks and employ those most appropriate to your system:

1. Increase the size of the connection queue.
2. Employ associated vendor patches that address SYN flooding.
3. Decrease the connection establishment timeout length.
4. Employ an intrusion detection product that detects and compensates for SYN flooding.
5. Employ operating system patches in order and in a timely manner to eliminate vulnerabilities that may result in your becoming a launching platform for a Denial of Service attack.

“This is Not a Hoax” and Other Hoaxes

Submitted by the Department of Education

“This is not a hoax.”

If you’ve ever seen such a line in an e-mail message, chances are the message was a hoax. Each year, hundreds of e-mail hoaxes are circulated all over the world. A cousin to the e-mail virus, a hoax damages computer systems by convincing many people to send the hoax message to everyone they know. When too many messages are sent, e-mail systems can overload, slow down and even crash.

How can you tell if the e-mail message you received is a hoax? The first clue is if the message states “This is not a joke” or something similar. The second clue is if the message contains a line asking you to pass the message along to everyone you know. Hoaxes are often written very cleverly, pretending to warn you about an imminent danger such as new virus or a new Internet scam. The hoax succeeds if it convinces you to e-mail many people about the “warning” or other message.

other reliable way to determine if the message you’ve received is a hoax is to check with a reputable hoax-verification Web site. These sites regularly monitor Internet hoaxes throughout the world and post lists of current and old hoaxes. Some reliable verification sites are:

http://www.symantec.com/avcenter/hoax.html
http://hoaxbusters.ciac.org
http://www.antivirus.com/vinfo/hoaxes/hoax.asp
http://urbanlegends.about.com/science/urbanlegends/library/blhoax.htm
http://vil.mcafee.com/hoax.asp

Just as you should never open an e-mail attachment if you don’t know what it is, you also should never pass on a mass e-mail warning without first verifying it. At ED, only trust virus warnings when they come from OCIO Security. OCIO Security gets the latest security alerts and will notify all users of any legitimate threat. If you receive a hoax message, please ignore it and do not pass it on.

A recent hoax that made the rounds at the Department advised users to delete an “infected” file from the computer. The only problem was, the file was an essential component of the operating system, and deleting it damaged the computer. If you have any questions or concerns about an infected file, please call the Help Desk and allow the technicians there to make any necessary repairs.

Thus, a perpetrator may launch “fire and forget” attacks that self-execute from compromised hosts leaving no clear trial back to the actual originator of the attack.

Nimda, which is “admin” backwards, was the first worm to infect both email clients and network servers; giving it potential to spread faster than Code Red or any previously seen variant. The Nimda worm not only threatens Microsoft Internet Information Servers on Windows 2000 and NT hosts, but also individuals running Microsoft Outlook or Outlook Express for their email client. Once the server is infected it will begin to scan for vulnerable systems on the local network. Infected workstations can cause the entire contents of the hard drive (e.g. C drive) to be available over the network. Nimda can also add an additional user account with administrative rights, or super user.

A computer can become infected through a variety of means including opening a malicious email attachment or using a browser with no security enabled while viewing an infected webpage. Preventing infections from worms such as Nimda requires a mixture of policy and technology. Network administrators and users must keep anti-virus products, operating system and browser software updated. Network administrators should monitor patches available from Microsoft and other vendors. System vulnerabilities can be corrected before an infection occurs.

If your system becomes infected by Nimda, or any other malicious code, contact FedCIRC as soon as possible. FedCIRC Operations Center will provide specific recommendations and advice to remove malicious code from your systems while maintaining critical operational functions, wherever possible.

Calendar of Events

FedCIRC Partners Meeting
Date: January 23, 2002
Location: Washington, DC
POC: FedCIRC
202-708-5060
http://www.fedcirc.gov

SANS Computer Security Bootcamp
Dates: February 9 - 14, 2002
Location: Monterey, CA
POC: SANS Institute
720-851-2220
http://www.sans.org/Bootcamp.htm

SANS San Diego ISO
Date: February 25 - March 1, 2002
Location: San Diego, CA
POC: SANS Institute
720-851-2220
http://www.sans.org/sandiegoISO.htm

GSA/FTS Network Services Conference
Date: April 15 - 18, 2002
Location: Orlando, FL
POC: Federal Technology Service (FTS)
703-631-6174
http://www.gsa-fts.com

Latest FedCIRC Advisories

FedCIRC Advisory FA-2001-37
Buffer Overflow in UPnP Service on Microsoft Windows

FedCIRC Advisory FA-2001-36
Microsoft Internet Explorer Does Not Respect Content-Disposition and Content-Type MIME Headers

FedCIRC Advisory FA-2001-35
Recent Activity Against Secure Shell Daemons

FedCIRC Advisory FA-2001-34
Buffer Overflow in System V Dereived Login

FedCIRC Advisory FA-2001-33
Multiple Vulnerabilities in WU-FTPD

FedCIRC Advisory FA-2001-32
Buffer Overflow in HP-UX Line Printer Daemon

FedCIRC Advisory FA-2001-31
Buffer Overflow in CDE Subprocess Control Services

FedCIRC Advisory FA-2001-30
Multiple Vulnerabilities in lpd

FedCIRC Advisory FA-2001-29
Oracle9iAS Web Cache vulnerable to buffer overflow

FedCIRC Advisory FA-2001-28
Automatic Execution of Macros

FedCIRC Advisory FA-2001-27
Format String Vulnerability in CDE Tool Talk

Welcome Aboard

Steve Chase, CISSP
Outreach Team Leader

Tiffannie Farrington
Computer Specialist

Janice Robinson-Wells, CISSP
Computer Specialist

The FedCIRC Bits & Bytes Newsletter

Editors
Corliss A. McCain
Trudy A. Hawkins

We welcome your input! To submit your related articles and notices for future issues, please contact FedCIRC at 202-708-5060. Deadline for submissions for the next issue is March 1, 2002. Articles may be edited for length and content. Back issues of this newsletter can be found on the FedCIRC website www.fedcirc.gov/docs.html

FedCIRC is sponsored by the Federal CIO Council and is operated by the General Services Administration/Federal Technology Service